

AO 106 (Rev. 11/10) Affidavit for Search  
Warrant

AUSA Stephanie Stern, (312) 469-6132

**FILED**  
**2/11/2025**

UNITED STATES DISTRICT COURT

THOMAS G. BRUTON  
CLERK, U.S. DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

In the Matter of the Search of:

Case No. 25m99

Kik user account daddycuckwife stored at  
MediaLab.ai Inc., further described in Attachment A

Ref. No. 2025R00010

**APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT**

I, Laurie A. Boskovich, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

**See Attachment A**

located in the Central District of California, there is now concealed:

**See Attachment A, Part III**

The basis for the search under Fed. R. Crim. P. 41(c) is evidence, instrumentalities, fruits, and contraband.

The search is related to a violation of:

*Code Section**Offense Description*

Title 18, United States Code, Sections 2252 and 2252A

possession, receipt, and distribution of child pornography

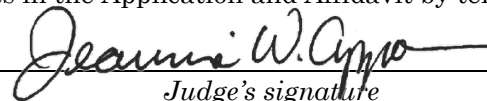
The application is based on these facts:

**See Attached Affidavit,**

Continued on the attached sheet.

/s/ Laurie A. Boskovich*Applicant's Signature*LAURIE A. BOSKOVICH, Special AgentFederal Bureau of Investigation*Printed name and title*

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: February 11, 2025*Judge's signature*City and State: Chicago, IllinoisJEANNICE W. APPENTENG, U.S. Magistrate Judge*Printed name and title*

UNITED STATES DISTRICT COURT            )  
  )  
NORTHERN DISTRICT OF ILLINOIS        )

**AFFIDAVIT**

I, Laurie A. Boskovich, being duly sworn, state as follows:

1.     I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately September 2017.

2.     As part of my duties as an FBI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in multiple forms of media, including computer media. I also have participated in the execution of multiple federal search warrants, many of which have involved child exploitation and/or child pornography offenses.

3.     This affidavit is made in support of an application for a warrant to search, pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with certain account(s) that are stored at the premises owned, maintained, controlled, or operated by MediaLab.ai Inc., a social network provider located at 1222 6th Street, Santa Monica, California 90401. The account to be searched is Kik user account daddycuckwife (the “**Subject Account**”), which is further described in the following paragraphs and in Part II of Attachment

A. As set forth below, there is probable cause to believe that in the account, described in Part II of Attachment A, in the possession of MediaLab.ai Inc., there exists evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 2252 and 2252A (the “**Subject Offenses**”).

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence, instrumentalities, fruits, and contraband of violations of the **Subject Offenses**, are located in the **Subject Account**.

## **I. BACKGROUND INFORMATION**

### **A. Kik Messenger**

5. Kik Messenger (“Kik”) is an application-based communication service owned by MediaLab.ai Inc. and headquartered in Santa Monica, California. Kik’s Guide for Law Enforcement describes Kik as a free smartphone messenger application that lets users connect with their friends and the world around them through chat. Kik uses smartphone data plans or Wi-Fi connection to send and receive messages to other Kik users, bypassing SMS (short message service). The Kik application is primarily used on a smart device, such as an Apple iPhone, Android cell phone, Apple iPad, or Android tablet. However, Kik can be used on any computing

device utilizing an emulator that can make a computing device look like an Android device.

6. A main attraction of Kik that differentiates it from other messaging apps is its anonymity. To register for the Kik service, a user must enter a first and last name, e-mail address, birth date, and select a username. Kik does not verify the information an individual enters, meaning users can create accounts using fake names, e-mail addresses, and/or birth dates if they so choose. Kik does not require a phone number for registration and uses usernames as the unique identifier. Usernames are unique and cannot be replicated, which affords users additional privacy. Although each username is unique, Kik users can create multiple accounts under different usernames and tied to different e-mail addresses.

7. Kik members can only see other Kik members' display names<sup>1</sup>, usernames, and profile pictures. Kik Messenger allows for group chats with up to 50 participants and facilitates real-time video chat options, which allow for live, private video chat for up to six people. Chats on Kik Messenger are not viewable remotely. Chats are only viewable with the user's password and from the device on which the application is stored.

8. After setting up a Kik account, the user can then post and share photographs and videos with other users on the platform. The user can also send private messages, photographs, and videos directly to another user. Because Kik

---

<sup>1</sup> A Kik user's display name is different from his or her username.

functions as a cloud service that stores messages, photos, videos, documents, and other files, users can access their data from any of their devices at any time without having to rely solely on local device or third-party backup storage. For this reason, a Kik user's content stored within the application, including stored messages, photos, and videos, may not be available within the specific application on an electronic device.

9. All data stored within Kik is heavily encrypted. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of MediaLab.ai Inc., to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow MediaLab.ai Inc. to make a digital copy of the entire contents of the information subject to seizure specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A.

## **II. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH**

10. In summary, and as set forth in more detail below, in approximately January 2025, PAUL A. GARCIA used Kik user account daddycuckwife (the "**Subject Account**") to send one image and three videos containing child sex abuse material ("CSAM") to an individual who, unbeknownst to GARCIA, was an FBI agent ("OCE-1") posing as a Kik user. GARCIA represented to OCE-1 that some of the images depicted his granddaughter. On or about January 31, 2025, GARCIA's daughter ("Individual A") was interviewed and confirmed that one of the (clothed) images that

GARCIA sent to the OCE-1 depicted her daughter, GARCIA's granddaughter, who is a 9-year-old female ("Minor 1"). Individual A further stated that the photograph appeared to have been taken in GARCIA's former residence in Texas, where Minor 1 lived with GARCIA until approximately 2020.

**A. GARCIA is the User of the Subject Account**

11. According to records provided by Kik on or around January 26, 2025, the registered email address for the **Subject Account** is pg190352@gmail.com. On or about January 25, 2025, at approximately 21:29:09 UTC, the **Subject Account** utilized IP Address 107.212.48.55.

12. According to publicly available information, the internet service provider for IP Address 107.212.48.55 is AT&T. According to information provided by AT&T on or around January 26, 2025, the subscriber for the AT&T account is "[Individual B]" at address 3744 South Langley Ave., Chicago, IL 60653.

13. According to information provided by Google, on or around January 27, 2025, the Google Pay information for email account pg190352@gmail.com listed the customer display name as "Paul Garcia." On or about May 13, 2023, a credit card was linked to the Google Pay account with the billing name of "Paul A. Garcia." On or about October 14, 2024, a credit card was linked to the Google Pay account with a billing name of "[Individual B]."

14. According to the Illinois Secretary of State, PAUL A. GARCIA was issued a temporary driver's license in the state of Illinois on or about December 20,

2024. Garcia's driver's license listed 3744 S. Langley Avenue, Unit 201, Chicago, IL as his address.

15. On or around January 27, 2025, the FBI requested the Chicago Police Department conduct a well-being check at GARCIA's address. The responding officer reported the following: [Individual B] and her 14-year-old son have been residing at 3744 South Langley Ave., Chicago, IL 60653 for approximately 10 years. Her boyfriend, GARCIA, also resides there. The responding officer observed no signs to indicate that a minor female child resides in the residence.

**B. Private Direct Messages with the Subject Account**

16. According to law enforcement reports, in or around January 2025, an FBI Online Covert Employee ("OCE-1") monitored a Kik group chat named, "Pantty Fetish VPL Creep see through and more." In or around January 2025, the **Subject Account** posted a video of an adult male rubbing a pair of panties on his penis to the group. After posting the video, OCE-1 sent a direct message to the **Subject Account** asking whose panties were in the video, and GARCIA responded to the effect that they belonged to his daughter. GARCIA then shared an image of an adult female and minor female together, advising OCE-1 that the image was of his daughter and granddaughter. GARCIA said his granddaughter was 8 years old.

17. According to law enforcement reports, the **Subject Account** showed it was 883 days old at the time of first contact.

18. As depicted below, the **Subject Account** used a profile picture that featured a brick wall.<sup>2</sup>



19. According to OCE-1, from approximately January 25, 2025, to approximately January 26, 2025, OCE-1 communicated with GARCIA, who was using the **Subject Account**, via private message through Kik.

20. According to law enforcement reports, during OCE-1's private message chat with the **Subject Account**, GARCIA told OCE-1 that he was a grandfather from Illinois with a 23 year-old daughter and an 8 year-old granddaughter. GARCIA described seeing his granddaughter nude and described her pubic region. GARCIA also told OCE-1 that he had an image depicting his semen on his granddaughter's face. GARCIA sent multiple videos and images that he described as being his granddaughter.

21. As further described below, Garcia sent various images and videos that he described as depicting his granddaughter, Minor 1:

---

<sup>2</sup> As described, the user of the **Subject Account** was later identified as GARCIA.



Subject Account	OCE-1
	Your wife and daughter are gorgeous. I'm sure your granddaughter will be too. Where are you from?
Illinois...Nnu...Fuck yes she maturing fast n sassy as fuck	
	Cali here...love a little sass...what you all into?
Truth open minded no bars hold	
	No limits here either...You into just your daughter or granddaughter too?
Mmmm granddaughter too b honest	
	I feel you...I am the same with my girl.
[Garcia sends two videos of a minor female child who is fully clothed. The child is laying on a bed.]	
	Oh fuck that your granddaughter?
Love play wrestling n cops n Robbers with her .. she loves play cop and Robbers so I can feel on her...Yes	
	Mmmmmm...How much have you gotten to feel?
[Garcia sends video file 24e05c6c-65d0-490f-95c2-cbc48f5aedef9 <sup>3</sup> depicting a minor female child who is fully clothed. There is a bed next to her with a quilt green and pink in color.]	
What about your daughter?	
	Mostly take creep shots and spy on mine...Play with her panties too
Felt everything more when she sleeping...All time...Cum in them	
	Yeah sleep time is the best...Ever taken nudes of her? Or your

<sup>3</sup> As described below, this image was shown to Individual A and identified as Minor 1.

	daughter? (OCE-1 sends image of panties on top of an adult foot).
Omg fuck yes...Mmmm she have pubes already	
	No not yet...What about yours?
<p>My granddaughter 8 she already starting sprout</p> <p>[Garcia sent a video of a fully clothed minor female child sleeping. She is wrapped in the same green and pink quilt that was present in the previous video. Someone approaches the sleeping child and takes the quilt off her]</p> <p>[Garcia sent an image depicting the bare chest of a minor child. The child's face is not visible, but it is apparent the child has long hair.]</p> <p>Nipple</p>	
	Mmmmm
<p>[Garcia sent a video of a fully clothed minor female child sleeping. The child is wrapped in the same green and pink quilt. Someone approaches the child and pulls down the back of her shorts revealing her buttocks to the camera.]</p> <p>Look risky...Tell me what you like to do...</p>	

22. According to OCE-1, in addition to the above video depicting an adult male hand pulling down the pants of a minor female revealing her buttocks, GARCIA also sent one image and one video depicting an adult hand pulling down the pants of

a minor female child, who GARCIA claimed was his granddaughter, revealing her anus and genitals:

Subject Account	OCE-1
<p>[Garcia sends image file 299ac7ce-3e3f-493c-9a6d-455e74500287.jpg, depicting an image of an adult's hand pulling down the waistband of a female minor's pants to reveal her vagina. Based on the size of the child's hips and thighs in comparison to the adult's hand, it is estimated the child is 8 to 10 years old. The child appears to have some fine pubic hairs.]</p> <p>Her pubes barely starting to flourish</p>	
	Fuckkk that's your granddaughter????
She only 8...yes my granddaughter	
	Mmmmmm fucking hot
Show me video of that cock...show me something nasty	
	(OCE-1 sends image)
Video...those are old pics huh...there you go	
	No recent
<p>[Garcia sends video file 480b48c8-90ab-4e47-b37d-42025f455cd4, showing an adult hand pulling down the waistband of a minor female child's shorts revealing her buttocks. The child appears to be laying face down. The adult hand uses one finger to spread the child's buttocks apart.]</p> <p>See you cock now...that's about 2 weeks old</p>	
	Mmmm so good...What's the dirtiest pic or vid you've gotten of her?

Pic my cum on her face	
------------------------	--

23. According to OCE-1, GARCIA also sent two apparently unrelated videos depicting CSAM.

a. Video file a5ac-2720-db5e-4008-8c47-2f6d2545bc88 is an approximately 25-second long video depicting an approximately 10-year old minor female child who is fully nude, with the exception of a black masquerade type mask. The child's mouth is wrapped around an adult's penis. At one point in the video, a male voice asks the child "how old are you again?" The child looks up and responds "10."

b. Video file 7a0aadb6-0e87-4841-a176-d9e1585189d2 appeared to be an approximately 40-second video depicting a minor female child under the age of 13 years old. The child is nude from the waist down and laying on a bed. The camera is positioned between the child's legs exposing her vagina and buttocks. The child rubs her vaginal region then lifts up her shirt exposing her chest to the camera.

24. After sending the two video files, Garcia stated "hope you like this lil girl."

**C. Interview of Individual A**

25. On or around January 31, 2025, GARCIA's adult daughter, Individual A, was interviewed by the FBI. In summary, Individual A reported the following:

a. Individual A has a 9 year-old daughter (Minor 1) who resided with her grandparents, Individual A's mother and father (GARCIA), in Texas until approximately 2020.

b. Individual A positively identified photographs of herself shared with OCE-1 by GARCIA.

c. A still shot image of video file 24e05c6c-65d0-490f-95c2-cbc48f5aedf9 was shown to Individual A. Individual A positively identified her daughter in the image. Individual A indicated the video was taken in GARCIA's house in Texas, as she recognized the background of the room.

26. A Child and Adolescent Forensic Interview of Individual A's 9 year-old daughter, Minor 1, is going to be scheduled for a later date.

### **III. SEARCH PROCEDURE**

27. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of MediaLab.ai Inc. to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to MediaLab.ai Inc. personnel who will be directed to the information described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, MediaLab.ai Inc. employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact

duplicate of all information stored in the computer accounts and files described therein;

c. MediaLab.ai Inc. employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

d. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records received from MediaLab.ai Inc. employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

#### IV. CONCLUSION

28. Based on the above information, I respectfully submit that there is probable cause to believe that evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 2252 and 2252A are located within one or more computers and/or servers found at MediaLab.ai Inc., headquartered at 1222 6th Street, Santa Monica, California 90401. By this affidavit and application, I request that the Court issue a search warrant directed to Other MediaLab.ai Inc. allowing agents to seize the electronic evidence and other information stored on the MediaLab.ai Inc. servers following the search procedure described in Attachment A and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.

/s/ Laurie A. Boskovich

Laurie Boskovich  
Special Agent  
Federal Bureau of Investigation

Sworn to and affirmed by telephone 11th day of February, 2025



Honorable JEANNICE W. APPENTENG  
United States Magistrate Judge

## **ATTACHMENT A**

### **I. SEARCH PROCEDURE**

1. The search warrant will be presented to MediaLab.ai Inc. personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. MediaLab.ai Inc. employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

### **II. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES OF MEDIA LAB.AI INC.**

To the extent that the information described below in Section III is within the possession, custody, or control of MediaLab.ai Inc., MediaLab.ai Inc. is required to disclose to the government the following information for the **Subject Account**, as defined in the affidavit:



1. All subscriber records to include registration, identity and contact information for user ID “daddycuckwife,” including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
2. All past and current usernames, display names, account passwords, and names associated with the users of the account(s);
3. The length of service (including start date) and the means and source of payments associated with the service (including any credit card or bank account numbers);
4. All IP logs and other documents showing the IP address, date, and time of each login to the account(s);
5. All data and information generated by or associated with the Kik user ID/account and profile page, including photographs, “bios,” profile backgrounds and themes of account(s), any postings, status updates, photographs, comments, networks or groups of which the user is a member, and information about the user’s access and use of the Kik application;
6. All Kik groups (JIDs) that the **Subject Account** has joined or been a part of;
7. All privacy and account settings for account(s);
8. All activity logs for the account(s) and all other documents showing the posts of the **Subject Account**;

9. All log data, including browser type, hardware model, operating system, referring web pages, pages visited, location, mobile carrier, device and application IDs, search terms and cookie information for account(s);

10. All photos and videos uploaded by the user ID and sent to other Kik users, and all photos and videos uploaded by any users which were received by the user ID, to include all metadata associated with this media;

11. Any and all communications to include private messages, instant messages or direct messages sent or received by users of the Kik account(s) including any and all content sent or received in the messages, date and timestamp of when content was sent or received and to whom it was sent or received, date and timestamp of the messages sent or received, and IP connection history when messaging;

12. All records of Kik searches performed by the Kik account from January 26, 2023 through the present; and

13. A listing of any and all groups, guilds or servers of which users of the account(s) are members.

Pursuant to 18 U.S.C. § 2703(d), the service provider is hereby ordered to disclose the above information to the government within 14 days of the signing of this warrant.

### **III. Information to be Seized by Law Enforcement Personnel**

All information described above in Section II that constitutes evidence, instrumentalities, and fruits concerning violations of Title 18, United States Code,

Sections 2252 and 2252A (the **Subject Offenses** as defined in the affidavit), as follows:

1. Items related to the identity of the user or users of the **Subject Account**;
2. Items related to the physical location of the users of the **Subject Account** at or near the times of the **Subject Offenses**;
3. Communications with suspected minors involving sexually-explicit materials, or the request for sexually-explicit materials in any format;
4. Items related to the identities and contact information of participants in or witnesses to the **Subject Offenses**;
5. Evidence indicating the **Subject Account's** account owner's state of mind as it relates to the crime under investigation;
6. The identity of the person(s) who created or used the **Subject Account**, including records that help reveal the whereabouts of such person(s);
7. All records, files, and documents, (including, but not limited to, photographs, images, videos), including all temporary and permanent electronic files and records (including, but not limited to, JPG, GIF, TIF, AVI, WAV, and MPEG files), that contain, attach, reference, or describe child pornography materials or visual depictions of minors engaged in sexually explicit conduct;
8. All materials and items that are sexually arousing to individuals who are interested in minors, but may not in and of themselves be obscene or which do

not necessarily depict child pornography and/or minors involved in sexually explicit conduct. Such material is commonly known as “child erotica” and includes, but is not limited to, written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, diaries about sexual contact with children, and fantasy writings;

9. All records and documents, containing, showing, referencing, or describing an offer to transmit or receive any child pornography materials and/or depictions of a minor engaged in sexually explicit conduct;

10. Records and information relating to communications with any suspected minors;

11. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

12. All files, documents, communications, images, videos, and contacts associated with the Kik user account(s) pertaining to transportation/travel to engage in illicit sexual conduct, the enticement of a minor child, the receipt and/or distribution of child pornography, production of child pornography, or transfer of obscene material to a minor; along with any evidence that would tend to show the true identities of the persons committing these offenses;

13. All activity logs and IP logs, including all records of the IP addresses that logged into the account; and

14. All account information, including:

- a. All registration, identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
- c. All privacy settings and other account settings;
- d. All registered devices and accompanying serial numbers and other identifying numbers to include dates of activation, registration, deactivation;
- e. All accounts linked by cookies; and
- f. All records pertaining to communications between Kik and any person regarding the user or the user's Kik accounts, including contacts with support services and records of actions taken.

## **ADDENDUM TO ATTACHMENT A**

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant requires the recipient of the warrant to copy and produce the contents of an electronic account so that they may be reviewed in a secure environment for information consistent with the warrant.

The account provider shall provide the government only data that fall within the criteria as described in Attachment A(II), which may either be the entire contents of an account or only a subset of an account.

The government's review of the data shall be conducted pursuant to the following protocol:

The government must make reasonable efforts to use methods and procedures that will locate only those categories of data, files, documents, or other electronically stored information that are identified in the warrant, while minimizing exposure or examination of categories that will not reveal the items to be seized in Attachment A(III).

The review of electronically stored information contained in the account described in Attachment A may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures that minimize the review of information not within the list of items to be seized as set forth in Attachment A(III):

- a. examination of categories of data contained in the account to determine whether that data falls within the items to be seized as set forth in Attachment A(III);
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment A(III);
- c. surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment A(III);
- d. opening or reading portions of files, and performing key word or concept searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment A(III); and

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment A(III).

Law enforcement personnel are not authorized to conduct additional searches for any information beyond the scope of the items to be seized by this warrant as set forth in Attachment A(III). To the extent that materials produced by the account provider pursuant to this search warrant contain evidence of crimes not within the scope of this warrant appears in plain view during the government's review, the government shall submit a new search warrant application seeking authority to expand the scope of the search prior to searching portions of that data or other item that is not within the scope of the warrant. However, the government may continue its search of that same data or other item if it also contains evidence of crimes within the scope of this warrant.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS**  
**PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by MediaLab.ai, and my title is \_\_\_\_\_.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of MediaLab.ai. The attached records consist of **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**

\_\_\_\_\_

\_\_\_\_\_.

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of MediaLab.ai, and they were made by MediaLab.ai as a regular practice; and

b. such records were generated by MediaLab.ai's electronic process or system that produces an accurate result, to wit:



1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of MediaLab.ai in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by MediaLab.ai, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature